IN THE SPCIFICATION

Please amend the paragraph beginning on page 1, line 15 to the following:

A method as mentioned above is disclosed in "Specification of the Bluetooth System", v1.0B, Dec. 1, 1999, Specification Volume 1 (Core), Part B, Baseband Specification (More information on ~~Bluetooth~~ BLUETOOTH can be found on http://www.bluetooth.com). In this Specification the ~~Bluetooth~~ BLUETOOTH link encryption is standardized. This link encryption is based on a symmetric cryptographic algorithm. The cryptographic keys as used in this algorithm are derived from a consumer device ID and an authentication process. An authentication process is a process which is used by a consumer device to prove to another consumer device that it is actually the device it tells it is. The authentication process as performed in the ~~Bluetooth~~ BLUETOOTH link encryption is designed to provide user privacy when the user communicates between two of his two devices. This is achieved in the following way: the user chooses which device(s) he trust and brings 'in close contact' his user device and another consumer device. These two devices must share a common cryptographic secret. It is the user's responsibility that no eavesdropper can tap into the exchange of messages and modify the message content. Another authentication session is performed in the ~~Bluetooth~~ BLUETOOTH link encryption when the user chooses a PIN code in order to ensure that no unauthorized person can use his ~~Bluetooth~~ BLUETOOTH device(s). The PIN code is used here to authenticate the user.

Please amend the paragraph beginning on page 2, line 9 to the following:

It is clear that when using the ~~Bluetooth~~ BLUETOOTH link encryption the user of the devices chooses which device he trusts. This link encryption is therefore not suitable in the situation in which the user is not trusted and can not be asked to play the role of trusted authority. This is, for example, relevant in the

case where it must be prohibited that the user can attach to the device and copy or get access to content, stored on this device, illegally

Please amend the paragraph beginning on page 2, line 19 to the following:

In ~~ether~~ order to achieve this object, the method in accordance with the invention is characterized in that the method further comprises the step of:

Please amend the paragraph beginning on page 2, line 24 to the following:

The invention is based on the recognition that the security requirements for suitable content protection measures differ essentially from the security requirements for suitable user privacy protection measures, as for example implemented in the ~~Bluetooth~~ BLUETOOTH link encryption. As stated above, this kind of link encryption is not suited for content protection as the user is not trusted and can not be asked to play the role of trusted authority. Content protection is, for instance, used when data is digitally transferred from a sending device to a receiving device to ensure that only an authorized receiving device is able to process or render the content.

Please amend the paragraph beginning on page 3, line 7 to the following:

The invention has as an additional advantage that the method according to the invention can be introduced while maintaining functionality if older consumer devices are used. This is for example important if the link encryption according to the ~~Bluetooth~~ BLUETOOTH specification is used, as, within the ~~Bluetooth~~ BLUETOOTH consortium, interoperability is regarded as an essential feature. Moreover ~~if~~ it provides interoperability between compliant and non-compliant consumer devices. Compliant consumer devices are devices that can ~~proof~~ prove to each other that they know a secret that is only made available to devices which, have been certified to adhere to predefined content and/or copy protection rules.

Please amend the paragraph beginning on page 5, line 1 to the following:

After activating a data communication link between consumer devices 1 and 2 (not shown), two independent authentication sessions 3 and 4, each comprising key generation, are performed between the consumer devices 1 and 2. The first authentication session 3 serves the purpose of protecting the users privacy, and is identical to the key set up already used in ~~Bluetooth~~ BLUETOOTH.

Please amend the paragraph beginning on page 5, line 6 to the following:

This ~~Bluetooth~~ BLUETOOTH technology provides peer-to-peer communication over a relatively short distance of approximately ten meters. The system provides security measures both at the application layer and at the link layer. The link layer security measures are described in Chapter 14 of the Baseband Specification as mentioned before. This chapter describes the way in which authentication takes place between ~~Bluetooth~~ BLUETOOTH devices and the generation of keys that can be used for encryption/decryption purposes. Four different entities are used for maintaining security at the link layer: a public address which is unique for each user (the 48-bit IEEE ~~Bluetooth~~ BLUETOOTH device address, BD_ADDR), a private user key for authentication, a private user key for encryption and a random number (RAND) of 128 bits. The encryption key can be used for content protection. The random number is different for each new transaction. The private keys are derived during initialization and are further never disclosed. Normally, the encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8-128 bits). The size of the encryption key is configurable, among others to meet the many different requirements imposed on cryptographic algorithms in different countries--both with respect to export regulations and authority attitudes towards privacy in general. The encryption key is entirely different from the authentication key (even though the latter is used when creating the former). Each time encryption is activated a new encryption key shall be generated. Thus, the lifetime of the encryption key does not

necessarily correspond to the lifetime of the authentication key. It is anticipated that the authentication key will be more static to its nature than the encryption key--once established the particular application running on the ~~Bluetooth~~ BLUETOOTH device decides when, or if, to change it. To underline the fundamental importance of the authentication key to a specific ~~Bluetooth~~ BLUETOOTH link, it will often be referred to as link key. The RAND is a random number that can be derived from a random or pseudo-random process in the ~~Bluetooth~~ BLUETOOTH unit. This is not a static parameter, it will change frequently. It is in the interest of a user to ensure that no unauthorized person can use his ~~Bluetooth~~ BLUETOOTH device(s). For this reason, the user may choose a PIN code. As such, a user may be expected to use the ~~Bluetooth~~ BLUETOOTH system as intended for purposes which, for instance, involve privacy.

Please amend the paragraph beginning on page 8, line 4 to the following:

- Compliant content source with SDMI content and compliant receiving device:

According to the recent SDMI Specification, SDMI content is allowed to be sent over links that are protected. As the ~~Bluetooth~~ BLUETOOTH specification defines a secure link encryption system, ~~Bluetooth~~ BLUETOOTH can be used to send SDMI content. High quality content can be used if the consumer devices is used are compliant, limited quality content can be used if at least one of the consumer devices is non-compliant.

Please amend the paragraph beginning on page 8, line 11 to the following:

In FIG. 2 a first practical implementation of the method according to the invention is shown. In this example the method is used in a communication system comprising a music installation 14 and a portable CD-player 15 and the user of the portable CD-player wishes to download some content stored in the music installation. After activating a data communication link between the devices, for example by using ~~Bluetooth~~ BLUETOOTH link encryption, a first authentication session 16 is performed between these two consumer devices. In

this authentication session the music installation proves to the user of the portable CD-player that it is the consumer device the user wishes to download music from and the portable CD-player authenticates itself to the music installation as a portable CD-player. Next, a second authentication session 17 is performed between these two consumer devices. In this authentication session the portable CD-player proves to the music installation that the portable CD-player is allowed to download the content, i.e. it must prove it is compliant and the music installation authenticates itself to the portable CD-player. If both authentication sessions are successful, the key-merge block used for decrypting the encrypted content from the music installation is generated and the music can be downloaded to the portable CD-player.

Please amend the paragraph beginning on page 8, line 11 to the following:

It must be noted that, although the embodiments are directed to use in the ~~Bluetooth~~ BLUETOOTH specification, the invention is not limited to the ~~Bluetooth~~ BLUETOOTH link encryption. Also the DECT security standard can be used in the method for secure data communication according to the invention. The invention is also not limited to wireless data communication, but can also be used in non-wireless ways of data communication, for example the Internet.